REMARKS

Reconsideration of this application as amended is respectfully requested. Claims 1-17, 19-21, 25-65, 69-84, 86, 87, 89-97 remain pending.

Claim Amendments

Claims 1, 7-12, 15, 92, 94, have been amended. "Any amendment that will place the application either in condition for allowance or in better form for appeal may be entered." MPEP 714.13. The applicants acknowledge the restricted nature of After Final Practice and request that the Examiner use his discretion to enter the amendments. The amendment adding "text-based" before "activation code" in claim 1 and claims 7-12, 92, 94, which depend from claim 1, makes the use of "text-based activation code" consistent throughout, which presents the rejected claims in a better form for appeal, and requires only cursory review by the Examiner because proper antecedent basis was of a "text-based activation code" anyway. The amendment adding "communication" before "device" in claim 15 clarifies antecedent basis for consistency, which presents the rejected claim in a better form for appeal, and requires only cursory review by the Examiner because proper antecedent basis was of a "communication device" anyway.

Claim Rejections

Claims 1-17 and 19-21 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2003/0120541 (Siann et al.), in view of U.S. Patent 6,859,535 (Tatebayashi et al.). Claims 25-65, 69-84, 86, 87, 89-97 are rejected under 35 U.S.C. §103(a) as being unpatentable over Siann et al., in view of Tatebayashi et al., and further in view of Examiner Official Notice.

The Alleged Prior Art

Siann et al.

Siann et al. apparently disclose a method and device for electronically providing electronic media content and advertising content includes a media player and electronic media content from

an electronic media content provider. The media player is electronically provided with the electronic media content via a first method of transmission. The media player is also electronically provided with advertising content, from an advertising content provider, via a second method of transmission. If necessary, the electronic media content is decrypted by the media player prior to the electronic media content being provided to the user. The media player electronically determines when advertising is to be played on the media player. Additionally, according to an embodiment, when the media player is disconnected from the first method of transmission, and the media player ceases to receive electronic media content via the first method of transmission, the media player is electronically provided with advertising content via the second method of transmission. (Abstract).

The Examiner asserts at page 3 of the Office Action that Siann et al. disclose generating a text-based activation code associated with the information obtained from the playback device, wherein the text-based activation code includes data from which rights information is verifiable by the system. The Examiner relies upon several paragraphs of Siann et al. and the applicants' specification. Specifically, the Examiner asserts at page 3 of the Office Action that:

Paragraph 39 [of Siann et al.] describes access data as, for example, an authorization code which is used to ensure that the media player can decrypt the content. Therefore, access data is used to permit execution of content (content being displayed) in the player device, which is the same as description of the activation code in the applicant's specification page 15 lines 8-12. Paragraphs 97-98 clearly shows that access data is used to control access using cryptographic techniques which verify the data and allow access if the rules are satisfied. Paragraph 100 teaches configuring and providing (generating) the access data based on information specific to the certain media player. This information must be received at the device which generates the activation code so that it could be used in generation of the code.

Siann et al. state in paragraph 39: "'Access data' refers to data, for example decryption keys, that is used to ensure that a media player can decode secured electronic media content. Access data can be in the form of decryption keys, authorization codes, or the like." As an initial matter, it should be noted that there is no suggestion in Siann et al. that the access data is text-based. Nor is there any reason why Siann et al. would wish to make the access data text-based, since the

access data is simply provided from one machine to another. The text-based access data issue is described in more detail later with reference to Tatebayashi et al.

Siann et al. provide a description of how to use access data (i.e., to decrypt content), and elsewhere Siann et al. provide no alternative embodiment showing that the access data is used in any other way. For example, in paragraph 80, Siann et al. state: "FIG. 1B illustrates another embodiment of the present invention that includes access data. FIG. 1B is similar to FIG. 1A with the addition of a coordination system 160 that provides access data 164. Access data 164 is provided to the media player 120 from a coordination system 160. The coordination system 160 is the system that oversees the providing of electronic media content and advertising content to the media players and in one embodiment oversees the payment of revenue from advertising content providers to electronic media content providers. Access data 164 allows the electronic media content 110 to be secure, such that the electronic media content 110 is useable only if the proper access data has been provided to the media player 120. By using access data, secure electronic media content is decrypted."

Based upon this teaching, the Examiner makes a logical leap to allege "[t]herefore, access data is used to permit execution of content (content being displayed) in the player device, which is the same as description of the activation code in the applicant's specification page 15 lines 8-12." Page 15, lines 8-12, of the applicants' specification states: "The phrase 'activation code' describes a part of a whole license, considered necessary and sufficient to permit execution of selected specific content by the specific player device. An activation code might be an entire license, a part thereof, or a transformation thereof (such as a transformation suitable for human reading or data entry)." There is no apparent reason why Siann et al. at the time the present application was filed would provide access data that is suitable for human reading or data entry. There is also no apparent reason why Siann et al. would refer to their access data (referred to only as a "decryption key" when actual use is described) would be used to describe a part of a whole license or a part thereof. Thus, the Examiner's assertion that the access data of Siann et al. is "the same as description of the activation code in applicant's specification page 15 lines 8-12" is without support in the cited prior art. The applicants respectfully request that the Examiner withdraw the assertion or provide an affidavit showing that the Examiner is able to make such an

assertion without the benefit of a prior art reference. When a rejection in an application is based on facts within the personal knowledge of an employee of the Office, the data shall be as specific as possible, and the reference must be supported, when called for by the applicant, by the affidavit of such employee, and such affidavit shall be subject to contradiction or explanation by the affidavits of the applicant and other persons. (See MPEP 2144.03 and 37 CFR 1.104(d)(2)).

The Examiner asserts at page 3 of the Office Action that "Paragraphs 97 and 98 [of Siann et al.] clearly shows that access data is used to control access using cryptographic techniques which verify the data and allow access if the rules are satisfied." It should be noted that paragraphs 97 and 98 describe nothing more than access data being used as a decryption key, and separate access rules. The applicants note that the Examiner is apparently trying to subtly shift the use of access data into something other than a decryption key, which is the only use Siann et al. illustrates for the access data, and, indeed, the use described in paragraph 97. Siann et al. describe using access data to decrypt content, and access rules to determine rights. These are distinct.

The Examiner asserts at page 3 of the Office Action that "Paragraph 100 teaches configuring and providing (generating) the access data based on information specific to the certain media player. This information must be received at the device which generates the activation code so that it could be used in generation of the code." However, paragraph 100 simply explains that access data and access rules can be delivered in a cryptographically secure manner, and perhaps to groups of playback devices. The Examiner's assertion that Siann et al. teach configuring and providing the access data based on information specific to the certain media player is at odds with the explicit language of Siann et al., which is:

> [0100] According to an embodiment, to provide flexibility in the use of cryptographic mechanisms for such security, access data storage device 436 contains tables of parameters which include an identification part and a cryptographic key part, such that both are used to deliver access data and access rules, and other information to the media player in a cryptographically secure manner. A further embodiment allows access rules, access data and other generalized messages to be delivered to the media player uniquely, by groups, or

> globally, according to how the identification parameters are defined, and how their associated key variable parts are employed. Some or all of such parameters are specific and/or confidential to a certain media player, groups of players, or other such combinations. The system is not limited to a particular cryptographic security solution, but instead, the use of media player identifications can be based upon "groupings," multi-variable key sets that can be used with such grouping identifications, and the basis for system security and trust requirements for communications over the first, second and third methods of transmission can be supported by parametric data stored in the media player to effect cryptographic levels of security.

Contrary to the Examiner's assertion, at paragraph 100, Siann et al. say nothing about generating the access data based on information specific to the certain media player. It is not true that "This information must be received at the device which generates the activation code so that it could be used in generation of the code." The access data storage device 436 seems to generate the access data distinctly from the media player.

The Examiner takes the position that the "media player" of Siann et al. is not a "playback device," but rather is a combination of a "playback device," a "transmission/reception device," and a "device to enforce the access rules." In this way, the Examiner believes that he can argue that communications to the "transmission/reception device" are "via a transport technique not including the playback device." However, the Examiner apparently relaxes this interpretation when applying the Tatebayashi reference, as is described below with reference to Siann/Tatebayashi.

The Examiner does not attempt to assert that Siann et al. disclose a text-based activation code or a user communicates at least a portion of the activation code to the playback device (the access data is directly transmitted to the media player), and relies upon Tatebayashi et al. to make up for the deficiency.

Tatebayashi et al.

Tatebayashi et al. apparently disclose the media inherent key storing unit 220 prestores an inherent key Ki, the conversion unit 230 generates an encrypted inherent key Ji from the inherent key read from the media inherent key storing unit 220, the random number generating unit 331 generates a random number R1, the encryption unit 252 generates an encrypted random number S1, the decryption unit 333 generates a random number R'1 from the encrypted random number R1, and the mutual authentication control unit 334 compares the random number R'1 with the random number R1 and, if the random number R'1 matches the random number R1, judges that the memory card 200 is an authorized device. If the memory card 200 and the memory card writer have successfully authenticated each other, the memory card writer encrypts a content using a decrypted inherent key. If the memory card 200 and the memory card reader have successfully authenticated each other, the memory card reader decrypts an encrypted content using the decrypted inherent key. (Abstract).

The Examiner asserts at page 4 of the Office Action that Tatebayashi et al. disclose at col. 5, line 64 to col. 6, line 10, "an embodiment where the user has to enter part of a key so the access to the content is allowed." However, Tatebayashi et al. disclose that a user can enter a password. As Tatebayashi explain, "The user key means a password that is determined by each user, is known only by the user, and is inherent in the user. Also, the user key is a combination of alphabets, numbers, and symbols." Col. 37, lines 61-65. Notably, the user key is not associated with information obtained from the playback device. It is made up by and is inherent in a user.

Siann et al. and Tatebayashi et al. Combined

As was described with reference to the cited references, Siann et al. and Tatebayashi et al. fail to disclose that which the Examiner has asserted they do, which allegedly corresponded to the elements of the claims. It follows that Siann/Tatebayashi also fails to teach each and every element of the claims.

Moreover, the combination would not work as described. Specifically, the Examiner has asserted that the playback device does not include a transmission/receiver device (allegedly the "media player" includes a "playback device," a "transmission/receiver device," and a "device to enforce the access rules," and therefore it is possible for Siann et al. to send the text-based

activation code to a communication device, via a transport technique not including the playback device). If this is so, then the text-based activation code of Tatebayashi et al., which is input directly to the "device to enforce the access rules" (see col. 52, lines 52-65, which was cited by the Examiner), is never provided to the "playback device" either. Rather, the user key is entered and combined to encrypt files, and the combined key and encrypted files are provided to the playback device. The playback device provides the combined key and the encrypted files to the access device and the user enters the user key to facilitate decryption. So, according to the Examiner's logic, the user in Siann/Tatebayashi never communicates at least a portion of the text-based activation code to the "playback device."

In any case, Tatebayashi et al. explicitly teach a user key that is a password associated with a user. The user key is not generated by a license server (or any other device), and the user key includes no data from which rights information is verifiable by the system.

The Alleged Prior Art Distinguished

To render a claim obvious, the Examiner must account for each and every element of the claim. Claim 1 includes the language:

receiving information associated with a playback device;

generating a text-based activation code associated with the information obtained from the playback device, wherein the text-based activation code includes data from which rights information is verifiable by the system;

sending the text-based activation code to a communication device, via a transport technique not including the playback device;

wherein, in operation, a user of the communication device communicates at least a portion of the text-based activation code to the playback device;

further wherein, in operation, the playback device uses at least a portion of the text-based activation code to obtain rights to the content.

As described above, Siann/Tatebayashi fail to disclose generating a text-based activation code. Siann/Tatebayashi fail to disclose an activation code that includes data from which rights

information is verifiable by the system. Siann/Tatebayashi fail to disclose sending the activation code, as claimed, to a communication device, via a transport technique not including the playback device. Siann/Tatebayashi fail to disclose, in operation a user communicates at least a portion of the activation code, as claimed, to the playback device. Siann/Tatebayashi fail to disclose using at least a portion of the text-based activation code to obtain rights to the content. For any of these reasons, claim 1 is allowable over the cited prior art, whether considered alone or in combination.

Claims 2-17, 19-21, 91-95, which depend from claim 1, are allowable at least for depending from an allowable base claim, and potentially for other reasons as well. For example, claim 12 includes the language, "at least a portion of the text-based activation code is provided to the playback device, wherein the playback device processes the portion of the text-based activation code and produces a licensing message suitable to be sent by the communication device." The Examiner asserts at page 8 of the Office Action that Siann et al. teaches this at paragraph 81. "Also, paragraph 90 describes content provider payments when users play their content or download the licensed content. This clearly implies a licensing message from user to content providers via Media Player. Note that per paragraph 95 the communication between the Media Player and Content Providers is two way." However, contrary to the Examiner's assertion, paragraph 81 says nothing about a licensing message suitable to be sent by the communication device. The Examiner says that paragraph 90 clearly implies a licensing message, but it does nothing of the sort. Paragraph 90 describes payments from advertisers; it has nothing to do with a licensing messages from a user of the media player. Also, paragraph 95 refers only to "any low band mobile wireless two way communication system in the art" but says nothing about actual two-way communications. So claim 12, and claim 13, which depends from claim 12, are allowable for additional reasons.

Claim 25 includes the language:

> generating a text-based activation code of a sufficiently small size that is convenient for a human to enter based on information associated with a playback device of a system;
>
> providing the text-based activation code via an SMS technique;

sending the text-based activation code in a text-based message to a hand-held device using an SMS technique, the text-based activation code including information from which rights information is verifiable by the system, wherein, in operation, a user of the hand-held device communicates at least a portion of the message to the playback device;

putting together, at the playback device, at least an identity of the playback device and an identity of content;

applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate execution rights for the playback device for the content, wherein the text-based activation code is not used to authenticate the execution rights;

verifying the execution rights using at least part of the text-based activation code as a cryptographic signature;

launching, when the execution rights are verified, content on the playback device in accordance with the execution rights.

For reasons similar to those described above with reference to claim 1, claim 25 is allowable over the cited references. The applicants note that although the Examiner has indicated Siann et al. disclose in paragraph 43 SMS as a possible "third method of transmission." However, Siann et al. disclose a list that is boilerplate in appearance, and never disclose an embodiment in which SMS is used, or would even make sense. Moreover, there is no suggestion that Siann et al. would be motivated to provide activation codes that are convenient for humans to enter. There is also no suggestion that the text-based activation code be sent to a hand-held device, and then be communicated to the playback device by a user. The Examiner simply refers to the rejection of claim 1, which does not specifically recite a hand-held device.

Regarding "verifying the execution rights using at least part of the text-based activation codes as a cryptographic signature," the Examiner refers to Siann et al. paragraph 98, and acknowledges that "Siann does not explicitly teach use of activation codes as a cryptographic signature. However, Siann teaches using cryptographic techniques, such as a license to verify authenticity. As a cryptographic signature is a cryptographic verification technique, which is well-known and widely practiced at the time of invention, it would have been obvious to the one skill in art to use

cryptographic signatures for verification. The motivation was to use a standard, commonly known and well developed technique to perform digital verification." The applicants respectfully disagree. The typical technique is to apply a hash function to data and encrypt with a private key to produce a signature for attachment to data. Digitally signed data is then separated into data, which is passed through a hash function, and the signature is decrypted using the signer's public key, and the hash of the data and the signature are supposed to match. It is not well-known to use part of a text-based activation code sent via SMS (or, more generally, a communication channel that does not include the playback device) and use it as a cryptographic signature for content on the playback device. The applicants respectfully request that the Examiner withdraw the rejection or either provide a reference that teaches "verifying the execution rights using at least part of the text-based activation codes as a cryptographic signature" as claimed, or provide an affidavit in accordance with 37 CFR 1.104(d)(2).

Claim 26, which depends from claim 25, is allowable at least for depending from an allowable base claim and potentially for other reasons as well.

Claims 27, 34, 35, 36, 69 are allowable for reasons similar to those described with reference to claim 25. Claims 28-33, 96, 97; 37-65; 70-84, 86, 87, 89, 90, which respectively depend from claims 27; 36; 69, are allowable at least for depending from an allowable base claim and potentially for other reasons as well.

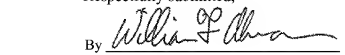
Conclusion

A Notice of Allowance is therefore respectfully requested. Should the Examiner find that a telephone or in-person conference would expedite the prosecution of this Application further, he is invited to contact the Applicants' counsel at the contact listed below for such a conference.

Please charge any deficiency in fees or credit any overpayment to our Deposit Account No. 50-2207, from which the undersigned is authorized to draw.

Dated: May 4, 2009

Respectfully submitted,

By 

William F. Ahmann
Registration No.: 52,548
PERKINS COIE LLP
P.O. Box 1208
Seattle, Washington 98111-1208
Attorney for Applicant